國泰航空公司

國泰航空有限公司就二零一八年十一月十三日信件中問題的回應

香港特別行政區立法會(“**立法會**”)要求國泰航空有限公司(“**國泰**”)書面回應葛佩帆議員所準備的問題。回應內容如下。

葛議員所提出的問題，部分涉及洩露與我們資訊系統安全相關的敏感信息。公開分享相關資訊會直接影響我們的資訊保安服務，從而增加對我們資訊系統和乘客個人數據安全的風險。因此，我們無法就下述有關問題提供詳細解答，我們先在此感謝葛議員的理解，亦要重申國泰正全面配合香港個人資料私隱專員以及香港警方對事件的調查。

1. 會否提交事故應變報告及調查報告，以公佈事發經過，及是次資料外泄的根本原因?

國泰正全面配合香港個人資料私隱專員對事件的調查，並已向公署提供有關是次數據洩露事件的詳細回應，包括事件的詳情以及我們能夠確定的根本原因。正如我們之前提到，由於涉及保安系統的敏感資料，公開該等資料會增加我們資訊保安的風險，故此我們未能在此分享相關資訊。

2. 有否在資料保管方面的差距分析，以知悉現時的合規情況，以及與有關法規（如：PCI DSS，歐盟一般資料保護規範，香港個人資料（私隱）條例）的差異程度?

國泰對其政策和程序進行定期審查，以確保我們遵守有關數據保護的法規和行業標準。 此類審查包括按最近引入的歐盟通用資料保護規則（GDPR），PCI DSS，以及過去就香港個人資料（私隱）條例的變更所進行的合規審查。

3. 會否提交現時的信息安全風險評估情況及安全影響分析，以及當在有同類事故的應對方法？

國泰有一套既定程序應對資訊系統安全及數據洩露事件。正如我們於二零一八年十一月十四日向立法會聯席會議保證，我們將審查有關程序，以確保我們能掌握從是次事件所吸取到的許多經驗教訓。

4. 如何進行整改計劃及內部信息安全服務水平協議，以應對所有可能發生的問題？

我們的整改計劃乃一套全面方案，並由一名方案經理專責統籌，在不同的項目經理支持下，定期實施，執行，跟踪，監測和報告工作方案的進展情況。

事實上，國泰已針對是次數據洩露事件實施了許多補救措施。當中有些為保護我們的防線及阻止黑客進入而在短期內已實行的措施，有些則為較長期及策略性的措施。

我們已封鎖了某些 IP 位址，關閉一些伺服器，並不時改變保護功能： 例如改變防火牆及對部分不尋常活動設定警報。我們亦已在整個網絡環境內設立進階威脅偵測系統。在調查過程中，我們亦同

時發展並馬上實施了多項策略性行動。這些行動包括擴展網絡分割及進一步改善網絡安全。我們一再強調，國泰的資訊系統一向都有健全的安全程序及安全防護，然而是次黑客使用了前所未見的惡意程式對我們的系統進行了十分精密而先進的攻擊。

5. 系統感染沒有識別碼病毒的過程及來源爲何?

我們在調查過程中，發現了攻擊者所使用的一些惡意軟件和實用程序。 這些惡意軟件或工具的識別碼前所未見，故此當時並未被我們所採用達行業最新標準的惡意程式偵測軟件檢視到。機於信息的敏感性，我們抱歉無法公開攻惡意軟件或實用程序列表。

6. 是否涉及安全監控系統失效，設置不當，或沒有覆蓋所有敏感資料系統，令病毒遲遲未被發現?

我們正全面配合香港個人資料私隱專員的調查，並已就我們的安全系統向公署提交詳細回應。 正如我們之前提到，由於該等資料涉及保安系統的敏感資訊，公開該等資訊會增加我們資訊系統保安的風險，故此我們遺憾未能在此公開分享。

我們希望籍此重申，國泰深明資訊系統的安全至關重要。在過去三年，我們在資訊系統基建和保安方面花費了超過十億港元。 國泰亦意識到，隨著黑客手段愈趨精密和先進，我們應對網絡安全威脅的反應亦需因時制宜，資訊技術保安的規劃上亦要不斷改良演變，包括強化壯大我們的資訊技術安全團隊以應付急速變化環境所帶來的挑戰。

7. 資料由什麼系統洩露: 如果是飛機上購買產品的系統，是否涉及第三方服務供應商？

是次事件涉及部分包含乘客數據的資訊系統。並沒有員工，飛行安全或操作系統受到影響。飛機上的銷售系統亦沒有受影響。

國泰航空有限公司

二零一八年十一月